UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,304	06/15/2000	Christopher E. Mitchell	777.395US1	9317

22801 7590 12/01/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/594,304	MITCHELL ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani, Ph.D.	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *25 June 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-13,15-16,19-33,35-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-13,15,16,19-33 and 35-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is responsive to the amendment filed on June 25, 2004, in which claims 1, 5, 11-13, 16, 27, 36, 37, 41 and 42 are amended, and claims 4, 14, 17, 18 and 34 are cancelled.

Claims 1-3, 5-13,15, 16, 19-33 and 35-42 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 5, 11-12, 37-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior arts of record, Brown et al. (U.S. Patent 6,678,733 and Brown hereinafter) in view of Moreau (U.S. Patent 6,609,954).

In regards to claims 1 and 5, Brown teaches a system for updating keys (i.e. the keymaster 442 provides encryption keys to the GS 416, WDPS 414, and Internet Server 418) (col. 10, lines 23-24) that decrypt login tickets (i.e. the WGPS decrypts the ticket using the key) (col. 3, lines 21-22) that log a user into multiple sites (i.e. if the client does not provide a ticket or the ticket is invalid, the WGPS denies the HTTP request) (col. 3, lines 4-5), the method comprising:

generating a first key having a first version number (i.e. timestamp) (i.e. the WGPS 414 uses the timestamp to determine the secret key used to encrypt the ticket) (col. 12, lines 56-58);

providing tickets encoded consistent with the first key (i.e. the resulting encrypted ticket is passed 624 to the client) (col. 12. line 38), the ticket having a version number corresponding to the first version number (i.e. other information, such as the IP address of the client 112 and a timestamp may also be stored in the ticket 800) (col. 12, lines 20-22);

generating a second key having a second version number (i.e. the keymaster 442 issues a new key to the servers 414, 416, 418 at the expiration of the previous key. Each key is preferably indexed so that the keys can be individually identified) (col. 10, lines 34-37); and

when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number to the second version number (i.e. the keymaster 442 occasionally shares 710 a secret key with the GS 416 and the WGPS 414 via an SSL connection. Returning to Fig. 6, the GS 416 preferably uses a symmetric encryption technique to encrypt 622 the ticket 800, T, with the shared secret key to produce an encrypted ticket, T'.) (col. 12, lines 23-38);

Brown does not teach that the key comprises key data and executable code for decrypting tickets.

However, Moreau discloses a cryptographic data integrity apparatus and method (col. 1, line 6-7).

Moreau teaches the use of a key in the form of an executable (col. 2, lines 23-32).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system (Moreau, col. 2, lines 23-32).

In regards to claims 11 and 12, Brown teaches a system for updating keys (i.e. the keymaster 442 provides encryption keys to the GS 416, WDPS 414, and Internet Server 418) (col. 10, lines 23-24) that decrypt login tickets (i.e. the WGPS decrypts the ticket using the key) (col. 3, lines 21-22) that log a user into multiple sites (i.e. if the client does not provide a ticket or the ticket is invalid, the WGPS denies the HTTP request) (col. 3, lines 4-5), the method comprising:

generating a new key with an incremented version number (i.e. timestamp) (i.e. the WGPS 414 uses the timestamp to determine the secret key used to encrypt the ticket) (col. 12, lines 56-58);

sending the new key to a partner site for use in decoding tickets with the incremented version number (i.e. the keymaster 442 provides encryption keys to the GS 416,WDPS 414, and Internet Server 418) (col. 10, lines 23-24);

updating key and version information for a login server (i.e. the keymaster 442 occasionally shares 710 a secret key with the GS 416 and the WGPS 414 via an SSL connection) (col. 12, lines 23-25); and

generating tickets decodable by the new key when an indication that a key having a previous version number has expired (i.e. the PS preferably encrypts the ticket with the encryption key received from the keymaster) (col. 3, lines 15-17). The Examiner considers a timestamp a type of incremented version number.

Brown does not teach that the keys comprise key data and executable code for decrypting tickets.

However, Moreau discloses a cryptographic data integrity apparatus and method (col. 1, line 6-7).

Moreau teaches the use of a key in the form of an executable (col. 2, lines 23-32).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system (Moreau, col. 2, lines 23-32).

In regards to claim 37 and 41, Brown teaches a system of logging on to multiple sites (i.e. a method and system that authenticates users and authorizes the users to access a walled garden of network services) (col. 2, lines 15-17), the method comprising: sending a first login ticket to a desired site (i.e. to access the walled garden 420, the client must present a "ticket") (col. 8, lines 13-14), wherein the login ticket is encrypted (i.e. the resulting encrypted ticket is passed to the client) (col. 12, line 38)to be decoded by a first key having a first version number (i.e. the WGPS uses the timestamp to determine the secret key used to encrypt the ticket. Then the WGPS 414 uses the secret key to decrypt the ticket) (col. 12, lines 56-58);

receiving an indication that the first key has expired (i.e. if the client does not provide a ticket or the ticket is invalid, the WGPS 3enies the HTTP request) (col. 3, lines 4-6);

obtaining a second login ticket from an authentication server (i.e. in response to a denial, the client sends a message to the GS requesting a ticket) (col. 3, lines 7-8), wherein the second login ticket is encrypted consistently with a new key having a second version number (i.e. the PS preferably encrypts the ticket with the encryption key received from the keymaster) (col. 3, lines 15-17); and

sending the second login ticket to the site to log into the site (i.e. then, the client sends the WGPS a new request to access a service in the walled garden and includes the ticket) (col. 3, lines 20-21).

Brown does not teach that the keys comprise key data and executable code for decrypting tickets.

However, Moreau discloses a cryptographic data integrity apparatus and method (col. 1, line 6-7).

Moreau teaches the use of a key in the form of an executable (col. 2, lines 23-32).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system (Moreau, col. 2, lines 23-32).

In regards to claim 38, Brown teaches that the tickets contain a version number which is readable without decryption (see figure 8, # 812). Brown also teaches that "in an alternative embodiment, the GS 416 encrypts only the portion of the ticket containing the bits representing the user access rights 816" (col. 12, lines 28-30).

In regards to claim 39, Brown teaches wherein the version number is a one digit Hex integer (i.e. the version number 812 is preferably a control number used by the GS 416 to ensure that the WGPS 414 properly interprets the ticket 800) (col. 12, lines 8-10). The Examiner infers from the above that the control numbers used by the GS 416 could thus include numbers consisting of one digit Hex integers.

In regards to claim 40, Brown teaches wherein the encrypted ticket comprises an unencrypted version number (see claim.38 above), and encrypted information sufficient to log a user into a desired site (i.e. access rights) (figure 8, #816) (i.e. in an alternative embodiment, the GS 416 encrypts only the portion of the ticket containing the bits representing the user access rights 816) (col. 12, lines 28-30).

In regards to claim 42, Brown teaches an encrypted ticket for use in logging on to a website (i.e. server), the ticket comprising:

an unencrypted version number (i.e. in an alternative embodiment, the GS 416 encrypts only the portion of the ticket containing the bits representing the user access rights 816) (col. 12, lines 28-30) corresponding to a key version number stored on the website; and

an encrypted string identifying the website and information (i.e. access rights) (fig. 8, #816) (i.e. other information, such as the IP address of the client 112 and a timestamp may also be stored in the ticket 800) (col. 12, lines 20-22), which when decrypted using the key having the same version number (i.e. the WGPS uses the timestamp to determine the secret key used to encrypt the ticket. Then the WGPS 414 uses the secret key to decrypt the ticket) (col. 12, lines 56-58) authenticates the user for logging the user into the website. The Examiner infers that such other information included in the ticket, in addition to the LP address of the client, could include the address of the website to be accessed.

Brown does not teach that the key comprises executable code for decrypting tickets.

However, Moreau discloses a cryptographic data integrity apparatus and method (col. 1, line 6-7).

Moreau teaches the use of a key in the form of an executable (col. 2, lines

23-32).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system (Moreau, col. 2, lines 23-32).

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brown in view of prior arts of record, See et al. (U.S. Patent 6,070,243 and See hereinafter) in further view of Curry et al. (U.S. Patent 6,237,095 and Curry hereinafter).

In regards to claim 2, Brown teaches the method of claim 1 as discussed above.

Brown, however, does not teach that a different key is provided to each site and that each key is encrypted for decoding at one site.

See discloses a system that relates to regulating connectivity to and communicability within communications networks (col. 1, lines 6-7). See teaches that a different key is provided to each site (i.e. preferably mutual authentication is accomplished through exchange of authentication keys configured on agent,100 and server 320) (col. 5, lines 45-47). The Examiner infers that the same concept of mutual authentication can be expanded to all other agents and servers thus establishing a different authentication key for each pair.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of See to include that a different key is provided to each site with. the motivation of combining the user-specific advantages of log-in challenges and the flexibility of VLANs into a deterministic user-based

authentication and tracking service for local users of institutional communication networks (See, cot. 2, lines 37-41).

The combination of Brown and See, however, does not teach that each key is encrypted for decoding at one site.

Curry discloses a method, apparatus and system for transferring money or its equivalent electronically. In particular, in an electronic module based system, the module can be configured to provide at least secure data transfers or to authorize monetary transactions (col. 1, lines 2528).

Curry teaches that a each key is encrypted for decoding at one site (i.e. He e-mails both the message encrypted with IDEA and the IDEA key encrypted with the user's public key to the user. No one that sees this transmission can read it except the intended recipient because the message is encrypted with IDEA and the IDEA key is encrypted with the intended recipient's public key) (col. 5, lines 37-41)

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown and See with the teachings of Curry to include that each key is encrypted for decoding at one site with the motivation of providing security from those who might try to read the user's email (i.e. tickets or messages) remotely (Curry, col. 5, lines 44-45).

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brown in view of See.

In regards to claim 3, Brown as modified teaches the method of claim 1 as discussed above.

Brown as modified does not teach further including generating a configuration file to track keys for each site.

See teaches generating a configuration file to track keys for each site (i.e. Means 540 serves to forward for storage and use by a network administrator user tracking information. User tracking information may include, for each login attempt, any information learned from one or more of the following: user identification information, authentication information, user status information, authorized communicability information) (col. 8, lines 49-65). The Examiner interprets "authentication information" as a type of information that might contain keys for each site.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of See to include generating a configuration file to track keys for each site with the motivation of combining the user-specific advantages of log-in challenges and the flexibility of VLANs into a deterministic user-based authentication and tracking service for local users of institutional communication networks (See, col. 2, lines 37-41).

In regards to claims 6, 9 and 10, Brown as modified teach, as discussed for claim 1 above, a method of generating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key having a first version number;

generating a second key having a second version number; and

providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

Brown does not teach that the key is in the form of an executable.

Moreau discloses a cryptographic, data integrity apparatus and method (col. 1, line 6-7). Moreau teaches the use of a key in the form of an executable (col. 2, lines 23-32).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system (Moreau, col. 2, lines 23-32).

In regards to claim 7, Brown teaches distributing the key to multiple login servers in a secure manner (i.e. preferably, the keymaster 442 has SSL links, or some other form of secure communication links, to the servers 414, 416, 418) (col. 10, lines 24-25).

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brown in view of Moreau as applied to claim 6 above, in further view of See.

In regards to claim 8, the combination of Brown and Moreau teaches the method of claim 6 as discussed above.

The combination of Brown and Moreau, as discussed for claim 6, does not teach updating a configuration file to track keys for each site.

See teaches updating a configuration file to track keys for each site (i.e. Means 540 serves to forward for storage and use by a network administrator user tracking information. User tracking information may include, for each login attempt, any information learned from one or more of the following: user identification information, authentication information, user status information, authorized communicability information) (col. 8, lines 49-65). The Examiner

interprets "authentication information" as a type of information that might contain keys for each site.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to further modify the combination of Brown and Moreau with the teachings of See to include updating a configuration file to track keys for each site with the motivation of combining the user-specific advantages of log-in challenges and the flexibility of VLANs into a deterministic user-based authentication and tracking service for local users of institutional communication networks (See, col. 2, lines 37-41).

Claims 13, 15, 16 and 18 are rejected tinder 35 U.S.C. 103(a) as being unpatentable over prior art s of record, Brown in view of Olkin et al. (U.S. Patent 6,584,564 and Olkin hereinafter).

In regards to claim 13, 16 and 18, Brown teaches a system of updating a key used to decrypt tickets used to log into a site, the method comprising:

receiving an updated key with a new version number (i.e. the keymaster 442 occasionally shares 710 a secret key with the GS 416 and the WGPS 414 via an SSL connection) (col. 12, lines 23-25);

making the updated key the current key (i.e. the WGSP 414 uses the timestamp to determine the secret key used to encrypt the ticket) (col. 12, lines 36-38)

Brown does not teach setting a time for an old current key having an old version number to expire.

Olkin discloses a system that relates generally to providing security for communications in networks such as the Internet (col. 1, lines 6-7). Olkin teaches setting a time for an old current key having an old version number to expire (i.e. The expiration setting 48d allows a sender 12 to

specify when the security server 24 (FIG. 1) should discard a message key, and thus make the secure e-mail 14 unreadable. The default will generally be to not explicitly force expiration, but after some substantially long period of time [perhaps years] the security servers 24 in most embodiments of the secure e-mail system 10 will probably need to do so.) (col. 9, lines 25-31).

The combination of Brown and Olkin does not at leach at least one of the keys comprise executable code for making the updated key the current key.

However, Moreau discloses a cryptographic data integrity apparatus and method (col. 1, line 6-7).

Moreau teaches the use of a key in the form of an executable (col. 2, lines 23-32).

It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of Olkin to include setting a time for an old current key having an old version number to expire with the motivation to minimally burden those using it (Olkin, col. 4, lines 33-34).

It would have been further obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown-Olkin with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system (Moreau, col. 2, lines 23-32).

In regards to claim 15, Brown teaches further comprising redirecting users attempting to log into the site using the old current key (i.e. If, for any reason, the GS 416 decides to invalidate or revoke a ticket, the GS 416 poisons the ticket by sending 712 an invalidity notice to the WGPS 414 as shown in FIG. 7. The WGPS 414 treats a request to access the walled garden 420 made by a client with a poisoned ticket as if no ticket had been included) (col. 12, lines 43-48).

The Examiner infers that it is reasonable to consider the use of the old current key as one of the reasons to invalidate or revoke a ticket. Brown further adds that "If the client does not provide a ticket or the ticket is invalid, the WGPS denies the HTTP request. In response to a denial, the client sends a message to the GS requesting a ticket. The user authenticates himself or herself to the client by providing authentication information and the client provides this information to the GS. Assuming the user is authenticated, the GS uses the PS to look up the user in the database and determine the services in the walled garden to which the user has access. Then, the GS constructs a ticket including a bit field indicating the user's access rights, an expiration date, and other information. The PS preferably encrypts the ticket with the encryption key received from the keymaster and transmits the encrypted ticket to the client." (col. 3, lines 4-18). In other words, the user is redirected to the GS for re-authorization.

Claims 19, 24 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior arts of record, Brown in view of Sherer et al. (U.S. Patent 6,115,376 and Sherer hereinafter).

In regards to claim 19 and 26, Brown teaches a system for managing keys used to decrypt tickets for logging onto a site, the method comprising:

receiving a first key with a first version number;

changing a current key variable to the first version number;

receiving a new key with an incremented version number; and identifying the new key as the current key.

Brown does not teach encrypting the first key and the new key using a hardware address. The instant application teaches that "encrypting the first key and the new key using a hardware

address" refers to "storing [the key] by fie site in encrypted form in a registry using a piece of information that is specific to the physical machine, such as the MAC address of the first network card" (page 10 lines 2-4).

Sherer teaches a system relating to security in the data networks and authentication of sources of data carrying a medium access control (MAC) layer address as a source address.

Sherer teaches storing a key using a piece of information that is specific to the physical machine, such as the MAC address (i.e. the star interconnection device stores, or otherwise has access to a certificate binding a MAC address on a port to a public key) (col. 7, lines 35-37).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teachings of Sherer to include encrypting the first key and the new key using a hardware address with the motivation of reducing many of the insecurities introduced by spoofing techniques (Sherer, col. 2, lines 48-49).

In regards to claim 24, Brown teaches wherein a new user using a previous version ticket (i.e. poisoned ticket) will be redirected to obtain a ticket corresponding to the new key following the new key being identified as the current key (i.e. If, for any reason, the GS 416 decides to invalidate or revoke a ticket, the GS 416 poisons the ticket by sending 712 an invalidity notice to the WGPS 414 as shown in FIG. 7. The WGPS 414 treats a request to access the walled garden 420 made by a client with a poisoned ticket as if no ticket had been included) (cot. 12, lines 4348). The Examiner infers that it is reasonable to consider the use of the old current key as one of the reasons to invalidate or revoke a ticket. Brown further adds that "If the client does not provide a ticket or the ticket is invalid, the WGPS denies the HTTP request. In response to a denial, the client sends a message to the GS requesting a ticket. The user authenticates himself or

herself to the client by providing authentication information and the client provides this information to the GS. Assuming the user is authenticated, the GS uses the PS to look up the user in the database and determine the services in the walled garden to which the user has access. Then, the GS constructs a ticket including a bit field indicating the user's access rights, an expiration date, and other information. , the PS preferably encrypts the ticket with the encryption key received from the keymaster and transmits the encrypted ticket to the client." (col. 3, lines 418). In other words, the user is redirected to the GS for re authorization.

Claims 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior arts of record, Brown in view of Sherer as applied to claim 19 above, in further view of Olkin.

In regards to claim 20, the combination of Brown and Sherer teaches the method of claim 19 as discussed above.

The combination does not teach setting a time for the first key identifying when such key may no longer be used.

Olkin teaches setting a time for the first key identifying when such key may no longer be used (i.e. The expiration setting 48d allovis a sender 12 to specify when the security server 24 (FIG. 1) should discard a message key, and thus make the secure e-mail 14 unreadable. The default will generally be to not explicitly force expiration, but after some substantially long period of time [perhaps years] the security servers 24 in most embodiments of the secure e-mail system 10 will probably need to do so.) (col. 9, lines 25-31).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown and Sherer with the teachings of Olkin to

include setting a time for the first key identifying when such key may no longer be used with the motivation to provide for highly secured communications (Olkin, col. 4, lines 26-27).

In regards to claim 21, the combination of Brown, Sherer and Olkin teaches the system of method 20. Olkin also teaches wherein a user currently logged in may continue to use the first key until the time expires (i.e. The default will generally be to not explicitly force expiration, but after some substantially long period of time [perhaps years] the security servers 24 in most embodiments of the secure e-mail system 10 will probably need to do so.) (col. 9, lines 28-31).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Brown, Sherer and Olkin to include wherein a user currently logged in may continue to use the first key until the time expires with the motivation to minimally burden those using it (Olkin, col. 4, lines 33-34).

In regards to claim 22, Brown teaches wherein a new user may only use a ticket corresponding to the second key when the second key is made the current key (i.e. the PS preferably encrypts the ticket with the encryption key received from the keymaster) (col. 3, lines 15-17). The Examiner interprets the above, to mean that the user can only encrypt a ticket with the key made current by the keymaster. In other words, the user can only encrypt or use a ticket corresponding to a second/new key once that key is made current by the keymaster.

Claims 23 is rejected under 35 U S.C. 103(a) as being unpatentable over prior arts of record, Brown in view of Sherer in further view of Olkin as applied to claim 20 above, in further view of Wasserman et al. (U.S. Patent 6,304,969 and Wasserman hereinafter).

In regards to claim 23, the combination of Brown, Sherer and Olkin teaches the method of claim 20 as discussed above.

The combination Brown, Sherer and Olkin does not teach setting the time to a reauthorization time determined by the site.

Wasserman discloses a system for verifying the authorization of a server to provide network resources to a client (see Abstract). Wasserman teaches setting the time to a reauthorization time determined by the site (i.e. when a security counter, or timer, exceeds the value of an expiration count stored at the client or at other selected times, an authorization interrupt is generated. The authorization interrupt eventually disables some or all of the functions of the client unless the server is authorized within an allotted period of time.) (col. 2, lines 48-57).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Brown, Sherer and Olkin with the teaching of Wasserman to include setting the time to a reauthorization time determined by the site with the motivation to verify the authorization of servers using a security system that cannot be readily accessed or overridden by an operator of the client system. (Waserman, col. 2, lines 2024).

Claims 25 is rejected under 35 U&C. 103(a) as being unpatentable over prior arts of record, Brown in view of Sherer as applied to claim 19 above, in further view of Audebert (U.S. Patent 5,937,068).

The combination of Brown and Sherer teaches the method of claim 19 as discussed above.

The combination does not teach teat the new key is identified as the current key by changing the current key variable to the second version number.

Audebert discloses a system and method for user authentication employing dynamic encryption variables (see Title).

Audebert teaches that the new key is identified as the current key by changing the current key variable to the second version number (i.e. The encryption can be performed with the aid of an encryption key which is preferably the value of the current dynamic variable Kn, although any other secret key Q [block 34] may alternatively be used) (col. 9, lines 46-50).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Brown and Sherer with the teaching of Audebert to include that the new key is identified as the current key by changing the current key variable to the second version number with the motivation to provide improved security against fraud. (Audebert, col. 4, lines 35-36).

Claims 27-28, 30-31, 33 and 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior arts of record, Brown in view of Audebert in further view of Kandansky et al. (U.S. Patent 6,295,361 and Kandansky hereinafter).

In regards to claim 27 and 36, Brown teaches a system of updating keys (i.e. the keymaster 442 provides encryption keys to the GS 416, WDPS 414, and Internet Server 418) (col. 10, lines 23-24) used to decrypt tickets (i.e. the WGPS decrypts the ticket using the key) (col. 3, lines 21-22) used to log into multiple sites on a network (i.e. if the client does not provide a ticket or the ticket is invalid, the WGPS denies the HTTP request) (col. 3, lines 4-5), the method comprising:

generating a new key with a new version number (i.e. timestamp) (i.e. the WGPS 414 uses the timestamp to determine the secret key used to encrypt the ticket) (col. 12, lines 56-58) to take the place of an old key with an old version number;

storing the new key on a site to b.- logged into by a user (i.e. the keymaster 442 provides encryption keys to the GS 416, WGPS 414, and Internet Server 418) (col. 10 , lines 23-24); and

redirecting new users to a login server to obtain a ticket consistent with new key (i.e. if the client does not provide a ticket or the ticket is invalid, the WGPS denies the HTTP request. In response to a denial, the client sends a message to the GS requesting a ticket. The user authenticates himself or herself to the client by providing authentication information and the client provides this information to the GS. Assuming the user is authenticated, the GS uses the PS to look up the user in the database and determine the services in the walled garden to which the user has access. Then, the GS constructs a ticket including a bit field indicating the user's access rights, an expiration date, and other information. The PS preferably encrypts the ticket with the encryption key received from they keymaster and transmits the encrypted ticket to the client.) (col. 3, lines 4-18).

Brown does not teach changing a current key indication to the new key.

Audebert discloses a system and method for user authentication employing dynamic encryption variables (see Title)

Audebert teaches changing a current key indication to the new key (i.e. The encryption can be performed with the aid of an encryption key which is preferably the value of the current dynamic variable Kn, although any other secret key Q [block 34] may alternatively be used) (col. 9, lines 46-50).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Brown with the teaching of Audebert to include changing a current key indication to the new key with the motivation to provide improved security against fraud. (Audebert, col. 4, lines 35-36).

The combination of Brown and Audebert does not teach allowing current logged in users to continue using the old key.

Kandansky teaches a method and apparatus to allow a key manager node in a network to initiate the process of changing a group key for all nodes in a multicasting group (see Abstract).

Kandansky teaches allowing current logged in users to continue using the old key (i.e. each receiver in the group uses both the new key and the old key for a predetermined time period or until all group members have received the key) (see Abstract).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Brown and Audebert with the teachings of Kandansky to include allowing current logged in users to continue using the old key with the motivation to provide a mechanism for a multicast key manager to change a group key used by all members in a group (Kandansky, col. 10, lines 27-29).

In regards to claim 28, Kandansky teaches wherein the old key may be used by current logged in users for a predetermined amount of time (i.e. each receiver in the group uses both the new key and the old key for a predetermined time period or until all group members have received the key) (see Abstract).

In regards to claim 30, Kandansky teaches wherein the predetermined amount of time may be set to zero to force all current and new users to login with a ticket consistent with the

new key version (i.e. each receiver in the group uses both the new key and the old key for a predetermined time period or until all group members have received the key) (see Abstract). The Examiner interprets the above to mean that time period could also be set to zero.

In regards to claim 31, Brown teaches wherein the ticket contains a version number (i.e. other information, such as the IP address of the client 112 and a timestamp may also be stored in the ticket 800) (col. 12, lines 20-22) consistent with the version number of the key, which can decrypt it (i.e. the WSPGS uses the timestamp to determine the secret key used to encrypt the ticket) (col. 12, lines 56-58). The Examiner interprets the timestamp to correspond to the version number.

In regards to claim 33, the combination of Brown, Audebert and Kandansky does not teach wherein a new key is generated based on a request of the site.

Audebert teaches wherein a new key is generated based on a request of the site (i.e. the first and second generator means respectively include third and fourth calculating means for producing at least a first of the dynamic variables according to a function involving the number of access requests formulated by the first unit prior to the current access request in progress. It follows from this particularly advantageous feature that by virtue of the present invention, the updating of a first one of the dynamic variables, which is used for example as an encryption key, need not be performed periodically and does not require, in the second unit or server, any recalculation or "making up" of the value of the dynamic variable calculated in respect of a prior access request, as compared with the current value of this calculated dynamic variable residing in the first unit at the time an access request is formulated.) (col. 5, lines 16-29).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to further modify the combination of Brown, Audebert and Kandansky with the teaching of Audebert to include wherein a new key is generated based on a request of the site with the motivation to provide improved security against fraud. (Audebert, col. 4, lines 35-36).

In regards to claim 35, Brown teaches wherein the keys are generated by an authentication server (i.e. keymaster), and are distributed to multiple login servers (i.e. GS, WGPS) for providing login tickets (i.e. the keymaster 442 occasionally shares 710 a secret key with the GS 416 and the WGPS 414 via an SSL connection) (col. 12, lines 23-25), (i.e. the user authenticates himself or herself to the client by providing authentication information and the client provides this information to the GS) (col. 3, lines 8-10). (Then the GS constructs a ticket) (col. 3, lines 13-14).

Claims 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over prior arts of record, Brown in view of Audebert in further view of Kandansky as applied to claim 28 above, in further view of Wasserman.

In regards to claim 29, the combination of prior arts of record, Brown, Audebert and Kandansky teaches the method of claim 28 as discussed above:
The combination of Brown, Audebert and Kandansky does not teach wherein the predetermined amount of time is no more than a reauthorization time by which a current user is normally required to provide login information.

Wasserman discloses a system for verifying the authorization of a server to provide network resources to a client (see Abstract). Wasserman teaches wherein the predetermined

amount of time is no more than a reauthorization time by which a current user is normally required to provide login information (i.e. when a security counter, or timer, exceeds the value of an expiration count stored at the client or at other selected times, an authorization interrupt is generated. The authorization interrupt eventually disables some or all of the functions of the client unless the server is authorized within an allotted period of time.) (col. 2, lines 48-57).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Brown, Audebert and Kandansky with the teaching of Wasserman to include wherein the predetermined amount of time is no more than a reauthorization time by which a current user is normally required to provide login information with the motivation to verify the authorization of servers using a security system that cannot be readily accessed or overridden by an operator of the client system. (Waserman, col. 2, lines 2024.

Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over prior arts of record, Brown in view of Audebert in further view of Olkin as applied to claim 27, in further view of Biran.

The combination of Brown, Audebert and Kandansky teaches the method of claim 27 as discussed above.

The combination of Brown, Audebert and Kandansky does not teach wherein keys are encrypted by the site using a hardware address, and stored by the site.

Biran discloses a system that implements memory protection (col. 1, line 7). Biran teaches wherein keys are encrypted by the site using a hardware address, and stored by the site (i.e. Protection block 48 also holds a numerical key 43 whose value is a function of a physical address 41 of register 40, as shown in a key-entry step 66. The physical address is determined by

the physical installation of I/0 adapter 38 in computer 46. Thus, the numerical key is hardware dependent and unique, since register 40 is assigned uniquely to application 34, and since register 40 has a unique hardware address.) (col. 6, lines 45-52).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Brown, Audebert and Kandansky with the teachings of Biran to include wherein keys are encrypted by the site using a hardware address, and stored by the site with the motivation of for ensuring fully non-contentious addressing between a plurality of applications and a memory (Biran, col. 2, lines 20-22).

Response to Arguments

Applicant's arguments in regards to claims 1-3, 5-13, 16, 19-33, 35-42 have been fully considered but they are not persuasive.

The Applicant argues that the claims as amended (referring to amended claims 1, 5, 11, 12, 13, 16, 27, 36,37, 41 and 42) now recite that " keys comprise executable code for decrypting tickets" and "at least one of the said keys comprise executable code for making the updated key the current key". The Applicant argues that none of the cited references teaches or suggests the claimed feature "keys comprising the code for decrypting ticket" or "for making the updated key the current key".

The Examiner responds that as stated in the statement of rejections of 1, 5, 11, 12, 13, 16, 27, 36, 37, 41 and 42 under U.S.C. 103(a), the claimed feature is taught by the secondary reference directed to Moreau. The Examiner infers that a key in executable form such as the one taught by Moreau would broadly constitute a key comprising executable code including a key

which embeds an executable code or an executable code which embeds a key, the key is considered executable, hence comprising executable code.

Action is Final

THIS ACTION IS FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be

obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.

Examiner

Art Unit 2131

E. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
A/U 2136